Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. In a computer system, a method for protecting sensitive information, the method comprising:
receiving input of sensitive information from a user;
computing a data shadow of the sensitive information for storage in a repository;
based on the data shadow stored in the repository, detecting any attempt to transmit the sensitive information; and
blocking any detected attempt to transmit the sensitive information that is not authorized by the user.

[c2] 2. The method of claim 1, wherein said sensitive information comprises structured data.

[c3] 3. The method of claim 2, wherein said data shadow is computed for the structured data as a regular expression and a hash.

[c4] 4. The method of claim 3, wherein said hash comprises a MD-5 hash.

[c5] 5. The method of claim 2, wherein said structured data includes credit card number information.

[c6] 6. The method of claim 2, wherein said structured data includes Social Security number information.

[c7] 7. The method of claim 3, wherein said regular expression represents formatting information for said structured data.

[c8] 8. The method of claim 3, wherein said hash is computed after normalization of the structured data.

[c9] 9. The method of claim 8, wherein said normalization includes removing any formatting information before computing the hash.

[c10] 10. The method of claim 1, wherein said sensitive information comprises structured data and said detecting step includes:
initially detecting said structured data by matching a format for that structured data.

[c11] 11. The method of claim 1, wherein said sensitive information comprises literal data.

[c12] 12. The method of claim 11, wherein said data shadow is computed for the literal data as a length value plus at least one hash of the literal data.

[c13] 13. The method of claim 12, wherein said at least one hash includes an additional first pass hash or checksum

value computed for the literal data.

[c14] 14. The method of claim 12, wherein said at least one hash includes a MD-5 hash computed for the literal data.

[c15] 15. The method of claim 1, wherein said at least one hash includes an optional checksum value computed for the literal data that allows relatively quick detection of the sensitive information and a MD-5 hash that allows subsequent verification.

[c16] 16. The method of claim 1, wherein said receiving input step includes:
receiving input indicating a type for the sensitive information.

[c17] 17. The method of claim 16, wherein said receiving input indicating a type includes:
receiving input indicating that the sensitive information is a password.

[c18] 18. The method of claim 16, wherein said receiving input indicating a type includes:
receiving input indicating that the sensitive information is a Social Security number.

[c19] 19. The method of claim 16, wherein said receiving input indicating a type includes:

receiving input indicating that the sensitive information is a credit card number.

[c20] 20. The method of claim 16, wherein said receiving input indicating a type includes:
receiving input indicating that the sensitive information is a personal identification number (PIN).

[c21] 21. The method of claim 1, further comprising:
automatically determining a type for the sensitive information that indicates formatting.

[c22] 22. The method of claim 21, wherein said step of automatically determining a type includes:
matching the input against a template for identifying a type.

[c23] 23. The method of claim 1, wherein said detecting step includes:
trapping an outbound buffer of data that may contain the sensitive information; and
in instances where the sensitive information comprises structured data, performing a regular expression search on the outbound buffer.

[c24] 24. The method of claim 23, further comprising:
if a regular expression match is found, normalizing data from the match so as to remove formatting and there-

after computing a hash on it, for comparison with corresponding hash values stored in the repository.

[c25] 25. The method of claim 24, wherein said hash is a MD-5 hash.

[c26] 26. The method of claim 1, wherein said detecting step includes:
trapping an outbound buffer of data that may contain the sensitive information; and
in instances where the sensitive information comprises literal data, performing a sliding window search on the outbound buffer.

[c27] 27. The method of claim 26, wherein said sliding window search includes performing an optional checksum calculation on successive blocks of bytes within the outbound buffer, for comparison with corresponding checksum values stored in the repository.

[c28] 28. The method of claim 27, further comprising:
if a match is found based on the checksum comparison, verifying the match with a MD-5 hash performed on data from the match.

[c29] 29. The method of claim 28, wherein said MD-5 hash performed on data from the match is compared against a corresponding MD-5 hash value stored in the repository.

[c30] 30. The method of claim 1, wherein said step of blocking includes:
referencing a stored policy indicating whether the sensitive information should be blocked from transmission.

[c31] 31. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

[c32] 32. A downloadable set of processor-executable instructions for performing the method of claim 1.

[c33] 33. In a computer system, a method for securing sensitive items from inappropriate access, the method comprising:
receiving input from a user indicating that a particular sensitive item is to be protected from inappropriate access;
storing metadata characterizing the particular sensitive item;
based on the stored metadata, detecting whether the particular sensitive item is present in any transmission of outgoing data; and
trapping any transmission of outgoing data that is detected to contain the particular sensitive item.

[c34] 34. The method of claim 33, further comprising:

a policy indicating what action the system should be taken upon trapping transmission of outgoing data that contains the particular sensitive item.

[c35] 35. The method of claim 34, wherein said action includes blocking any trapped transmission.

[c36] 36. The method of claim 34, wherein said action includes querying the user about whether the particular sensitive item may be transmitted.

[c37] 37. The method of claim 33, wherein said metadata includes a one-way hash of the particular sensitive item.

[c38] 38. The method of claim 37, wherein said one-way hash comprises a MD-5 hash.

[c39] 39. The method of claim 33, wherein said particular sensitive item comprises structured data, and wherein said metadata includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data.

[c40] 40. The method of claim 39, wherein said trapping step includes:

locating the particular sensitive item by first performing a regular expression search on the outgoing data for

finding a match based on formatting; and
for any match found based on formatting, performing a hash on the match to determine whether it matches a corresponding hash stored as part of the metadata.

[c41] 41. The method of claim 33, wherein said particular sensitive item comprises literal data and wherein said metadata comprises as a length value plus at least one hash of the literal data.

[c42] 42. The method of claim 41, wherein said trapping step includes:
locating the particular sensitive item by first performing a sliding window search through the outgoing data for a block of bytes having a size equal to said length value and having a hash value equal to one of said at least one hash of the literal data.

[c43] 43. The method of claim 42, wherein said at least one hash includes a MD-5 message digest computation.

[c44] 44. The method of claim 43, wherein said at least one hash further includes an optional first pass hash or checksum as an optimization.

[c45] 45. A computer-readable medium having processor-executable instructions for performing the method of claim 33.

[c46] 46. A downloadable set of processor-executable instructions for performing the method of claim 33.

[c47] 47. A system providing security for sensitive information, the system comprising:
a data processing system receiving input of sensitive information;
a secure lockbox module for storing a secure descriptor characterizing the sensitive information; and
a security module for detecting, based on said secure descriptor, any attempted transmission of outgoing data that contains the sensitive information.

[c48] 48. The system of claim 47, wherein said input includes an indication of a type for the sensitive information.

[c49] 49. The system of claim 48, wherein said indication of a type includes a selected one of structured data and literal data.

[c50] 50. The system of claim 49, wherein said structured data includes a credit card number.

[c51] 51. The system of claim 47, further comprising:
a security policy specifying what action is to be undertaken when the security module detects an attempt to transmit the sensitive information.

[c52] 52. The system of claim 51, wherein said security policy specifies an action of blocking any attempted transmission of the sensitive information.

[c53] 53. The system of claim 51, wherein said security policy specifies an action of prompting a user to allow or deny any attempted transmission of the sensitive information.

[c54] 54. The system of claim 47, wherein said sensitive information includes structured data, and wherein said secure descriptor includes regular expression information characterizing a particular format for the structured data and includes a hash computed on unformatted data extracted from said structured data.

[c55] 55. The system of claim 47, wherein said sensitive information includes literal data and wherein said secure descriptor includes a length value plus at least one hash of the literal data.